---

Topics:

## Outsourced IT Services and Third-Party Interconnections [1]

SS-08-044 Outsourced IT Services and Third-Party Interconnections

Issue Date: 03/31/2008

Revision Effective Date: 03/21/2008

# PURPOSE

Third party access to State computing resources is a common practice that presents potential security risks to the enterprise that must be examined and addressed. Two significant types of access are a network-to-network connection that allows multiple users or systems from a third party to interact with State resources and privileged access given to a third party to develop software or maintain systems. Managing the risks involved in these situations is something that must be done prior to making the connections available and requires that additional provisions be incorporated into service contracts.

This standard establishes the requirement for agencies to establish and document detailed security and operational requirements for third-party information system service providers and interconnections and monitor them for compliance.

# STANDARD

Granting access to state information systems by third parties shall been driven by a business need. The management of the associated risks is the responsibility of the State agency that is sponsoring the third party access.

Third-parties shall be provided with a copy of the State information security policies and standards as well as applicable agency security policies and procedures.

Third-party providers of IT services and/or connected partners shall be subject to the same security policies and procedures as the supported organization and shall conform to the same security controls and documentation requirements as they apply to the agency?s internal systems.

Any outsourcing agreement shall contain security provisions specifically tailored to the particular outsourcing initiative.

Access by and interconnections with Third Party networks or systems shall require a signed contract and /or a system interconnection security agreement that documents a complete understanding of what access exists, its usage and user profiles. The technical details of the connection shall include but is not limited to:

- A description of the need and services offered/obtained through the connection
- Information exchange and data flow diagrams , topological drawing, and controlled interface specifications
- Locations, description and examination of the third-party?s system/network security controls documentation, policies and procedures to identify risks to state resources.
- User profiles and access control descriptions
- Trusted behavior expectations and non-compliance implications
- Administrative communications requirements

It shall be responsibility and the right of the sponsoring agency to monitor outsourced information system service